Information Security Needs for the Electric Power and Other Process Industries

March 7, 2001

Joe Weiss
Technical Manager, EPRI EIS Program
650-855-2751
joeweiss@epri.com

EPRI EIS
Enterprise Infrastructure Security

Operational Systems

- Highly reliable, real-time systems that require secure two-way communication of dynamic data
  - Examples include Distributed Control Systems (DCS), Programmable Logic Controllers (PLC) and Supervisory Control and Data Acquisition (SCADA) Systems
- Operational systems designed to maximize performance and flexibility
  - Electronic security was not a significant consideration
  - Electronic security technology can inhibit performance
- Legacy systems assumed not to be vulnerable
  - Web-based applications can make them vulnerable
- Open systems can be vulnerable

Operational Systems (cont)

- E-commerce information security technology assumed directly applicable
  - Firewalls, intrusion detection, encryption, etc
  - Backfit of this technology could adversely impact system operation
- IT security policies and procedures assumed to apply to operational systems
  - Unique attributes of real time systems are often not addressed
- Technical expertise assumed readily available
  - Very few experts in both information security and real time systems

Vulnerable Hardware

- Process Plant and Electrical Generation Stations
  - Plant Distributed Control Systems (DCS)
  - Programmable Logic Controllers (PLC)
  - Field devices
  - Maintenance systems
- Transmission & Distribution (T&D) and Customer Facilities
  - Supervisory Control and Data Acquisition (SCADA)
  - Energy Management Systems (EMS)
  - Remote Terminal Units (RTU)
  - Protective Relays and Intelligent Electronic Devices (IED)
  - Automated meters
  - Power quality meters

Vulnerable Software /Protocols

- Operating Systems
  - NT, 2000, Linux, Unix, Solaris
- Fieldbus, MODBUS, and other buses
- Vendor Software
- Protocols
  - Inter Control Center Protocol (ICCP-TASE.2)
  - Common Information Model (CIM)
  - DNP
  - CORBA

Other Concerns

- ActiveX
- X-Windows
- PCAnywhere
- SSL
- Telecom and other communication media
- Uniform Computer Information Transaction Act
  - (UCITA)

Electric Company Vulnerability Assessment

- Conducted by 4 National Labs and consultant
- Able to assemble detailed map of perimeter
- Demonstrated internal and end-to-end vulnerability
- Intrusion detection systems did not consistently detect intrusions
- X-Windows used in unsecured manner
- Unknown to IT, critical systems connected to internet
- Modem access obtained using simple passwords
- Located many internal mission critical systems
  - DCS, SCADA, Call Management Systems

Paper Company Vulnerability Assessment

- Conducted by internal IT organization
- Self Assessments
- Vulnerability Scans
  - Modem hunt
  - Run scripts against Internet interfacing device
- Preliminary Results
  - Found connected modems to control systems unknown to IT
  - Used PCAnywhere on DCS console without password access
  - Once able to penetrate open console, ability to navigate network to systems at other plant locations

Open Issues/Recommendations

- Existing general purpose security products may not be applicable for process control applications
  - Need to investigate
  - If required, develop appropriate technology
- Basic information security requirements need to be developed for process control systems
  - Extend the Common Criteria
  - Existing equipment standards/requirements need to be reviewed to meet information security requirements
- Marry information security technology with process control technology
  - Neither can solve the problem in a vacuum